Regular paper http://dx.doi.org/10.13067/JKIECS.2014.9.10.1125

혼돈계의 단방향 동기화를 이용한 보안 프로토콜 설계

조창호* · 임거수**

Encryption Communication Protocol Design Using Unidirectional Synchronization of the Chaos System

Chang-Ho Cho* · Geo-Su Yim**

요 약

네트워크의 속도가 향상 되면서 정보를 담고 있는 콘텐츠의 양과 질이 급격히 증가 하고 있다. 이런 정보의 급격한 변화에 맞추어 콘텐츠를 통신상에서 보호할 수 있는 혼돈신호를 이용한 새로운 통신 프로토콜을 다음과 같이 제안한다. 혼돈시스템은 초기치 민감성과 발생된 신호가 잡음과 유사하여 예측이 불가능한 특성을 가지고 있다. 우리는 이런 특성을 갖고 있는 두 개의 혼돈시스템 $F(X_{n,}Y_{n})$와 $G(A_{n},B_{n})$를 구성하고 F 혼돈시스템의 신호로 G 혼돈시스템을 동기화시켜 발생되는 동일한 혼돈신호를 대칭키로 사용하고, 이렇게 구성된 암호 채널로 데이터를 송수신 하는 방법을 설계 하였다. 제안된 방법을 검증하기 위해 이미지의 암호화 및 복호화로 그 결과를 보였다. 우리가 제안한 방법은 기존의 암호화 통신과 다른 방법으로 추후 관련 분야의 연구에 초석이 될 것으로 생각된다.

ABSTRACT

The quantity and quality of contents containing information are sharply increasing with the rising network speed. In line with this rapid growth of information volume, a new communication protocol using the chaotic signal that can protect contents in communication is proposed as follows. The chaos system has the characteristic of unpredictability due to the sensitive initial values and the similarity of the signals with noise. We configured two chaos systems $F(X_{n,}Y_{n})$ and $G(A_{n},B_{n})$ that have such characteristics and designed a data communication method using as encryption channel the same chaos signals generated by synchronizing the chaos system G with the F signals. The proposed method was verified with the encryption and decryption of images. The proposed method is different from the existing encrypted communication methods and is expected to lay the foundation for future studies in related areas.is an example of ABSTRACT format.

키워드

Encryption, Decryption, Secure Channel, Chaos, Pseudorandom Number
암호화, 복호화, 보안채널, 혼돈, 유사난수

* 배재대학교 전기공학과(cho51111@pcu.ac.kr)
** 교신저자(corresponding author) : 배재대학교 전기공학과(lomac@pcu.ac.kr)
접수일자 : 2014. 08. 28 심사(수정)일자 : 2014. 09. 25 게재확정일자 : 2014. 10. 17

Ⅰ. 서 론

최근에 들어 네트워크의 속도와 관련기기들의 발달로 통신으로 전송되는 데이터의 양이 기하급수적으로 늘어나고 있다. 이런 대량의 데이터가 움직이는 정보화 사회에서 안전하게 데이터를 전송하기 위하여 통신방법에 관련하여 암호화, 보안채널, 보안라우팅에 대한 많은 연구 결과가 발표되고 있다[1-3]. 우리는 이런 연구결과와 더불어 다음과 같은 통신 보안에 관련된 결과를 제안한다. 우리가 제안하는 대칭키 암호화 방법은 보안에 사용되는 암호화 방법이 기존의 복잡한 알고리즘을 사용하는 DES(Data Encryption Standard)와 다르게 혼돈시스템의 복잡성을 적용한 방법으로 혼돈시스템의 구조에 따라 그 암호화 강도를 조절할 수 있어 효율성이 높다고 할 수 있다[4-6]. 혼돈시스템을 이용한 암호화 방법은 아직 많은 검증이 이루어지지는 않았지만, 새로운 방법으로 연구가 지속적으로 이루어진다면 좋은 결과가 있을 것으로 예상된다. 우리가 제시하는 암호화 방법은 혼돈신호의 특성을 이용한 암호화 방법이다. 이 와 같은 방법은 이미 많은 연구자들에 의해 연구가 이루어지고 있다. 우리는 이런 혼돈계의 특성중 동기화를 이용한 암호화 방법으로 네트워크의 정보를 보호 및 인증하는 프로토콜을 제안 하려고 한다. 혼돈시스템에서 발생하는 복잡한 신호는 인위적으로 복잡성을 구현한 것이 아니라 혼돈시스템의 내재적인 특성에서 발생되므로 신호발생 속도가 다른 암호화 방법에 비해 빠르고 시스템 구현이 용이하다. 또한 혼돈계의 비선형적인 특성이 암호화의 킷값으로 작용하기 때문에 혼돈계의 구조를 정확히 파악하기 전에는 암호화된 신호를 무단 복호화 하는 것은 불가능하다. 이런 특성으로 혼돈시스템을 이용한 암호화 방법은 다른 암호화 방법들과 같이 견고하다고 할 수 있다[7-9].

Ⅱ. 관련연구

2.1. 혼돈시스템의 특징

혼돈시스템은 비선형 복잡시스템의 대표적인 형태로 비연속적인 결과 값을 생성하는 계차방정식 구조와 연속적인 결과 값을 생성하는 미분방정식형태로 크게 나누어진다. 데이터 통신의 암호화에 효과적인 특성을 가지고 있는 계차방정식 혼돈시스템은 1차원 방정식의 Gauss-map, Logistic-Map, Tent-Map등이 있고, 2차원 방정식으로는 Henon-map, Ikeda-Map, Duffing-map 등이 있다[10-11].

위와 같은 계차 방정식 혼돈시스템의 성질은 이전 결과 값 x_n에 의해 다음 결과 x_{n+1} 값이 계산된다는 특징을 가지고 있고 이것은 단방향 인증이 가능하여 통신 보안에 효과적으로 적용 할 수 있는 특징이기도 하다. 이런 혼돈신호의 대표적인 다른 특징으로는 초기치 민감성과 유사 난수성질을 들 수 있다. 혼돈시스템에서 발생 되는 신호는 초기 값의 작은 차이가 이후 서로 연관성이 없는 다른 값으로 계산되는 특성을 가지고 있다. 이런 특성을 초기치 민감성이라고 하고 관련 내용을 그림 1에 보인다[12-14].

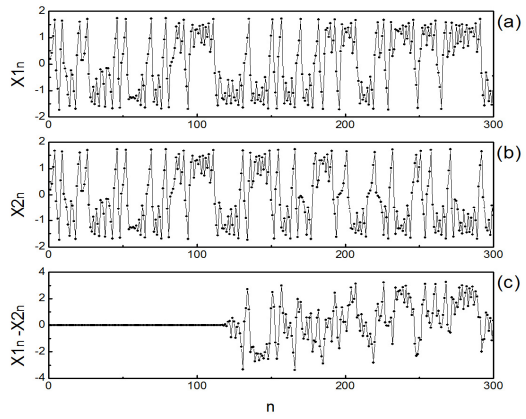

그림 1. 혼돈시스템의 시계열 그래프
Fig. 1 Temporal behavior of chaotic system

그림 1에 보인 혼돈시스템 시계열은 우리가 제안하는 프로토콜에 사용된 Duffing-Map의 시계열 결과 값이다. 그림에서 (a)와 (b)는 같은 초기 값으로 계산된 $X1_n$값과 $X2_n$값의 시계열이다. n값이 100을 지날 때 두 값에 대하여 $1.0E-5$의 오차를 주어 두 시계열의 변화를 확인 하였다. 초기에는 변화가 없으나 미세한 차이로 인하여 계산이 진행 되며 서로 상이한 값으로 변하는 것을 확인 할 수 있다. 이것은 전송되는 데이터가 무단으로 변조 되었을 때 변조의 유무를 확인 할 수 있는 장점이기도 하다. 또한 (a)와 (b)에서 보이는 시계열은 잡음과 유사한 특성을 가지고 있어 도청공격시 유출된 신호로는 전송되는 정보를 추

출 할 수 없는 특징을 가지게 된다.

2.2. 혼돈시스템의 암호화 방법

혼돈시스템의 신호를 이용하는 기존의 대표적인 암호화 방법은 CKBA(Chaotic Key-based Algorithm)방법으로 혼돈시스템의 특징 중에 하나인 초기치 민감성을 암호화에 적용 시킨 방법이다. 혼돈시스템에서 발생되는 신호의 특성은 잡음과 유사하다. 그러나 잡음은 재생산이 불가능 하지만 혼돈신호는 초깃값과 혼돈시스템의 상태를 처음과 같게 한다면 잡음과 유사한 같은 신호를 재생산 할 수 있는 특징을 갖고 있다. 이런 특성으로 혼돈신호를 결정된 잡음 이라고 한다. 이후 CKBA의 문제점을 보완하여 암호화 강도를 높인 방법인 CBFSC(Chaos-Based Feedback Stream Cipher)방법과 ECBFSC(Efficient Chaos-Based Feedback Stream Cipher)등이 발표 되었다[15-17].

우리는 이 방법들을 기초로 하여 통신에 적용시킬 수 있는 단방향 동기화를 이용한 보안 프로토콜을 다음과 같이 제안 한다.

III. 제안 프로토콜

3.1. Duffing Map 혼돈시스템

혼돈시스템의 단방향 동기화를 이용한 보안 프로토콜을 설계하기 위해 2차원 계차방정식 중 Duffing-Map을 사용하였고, 그 내용을 식 (1) 에 보인다.

$$x_{n+1} = y_n \qquad (1)$$
$$y_{n+1} = -bx_n + ay_n - y_n^3$$

우리가 제안한 보안 통신 프로토콜은 Duffing-Map 방정식 중 x_{n+1}과 y_{n+1}값을 각각 동기화와 암호화에 사용될 대칭키로 사용 한다.

식 (1)의 매개변수 a, b는 혼돈시스템의 특성을 결정짓는 값으로 암호화의 비밀키로 사용 된다.

Duffing-Map의 특성을 파악하기 위해 $a=2.77$, $b=0.17$로 각각 설정하고 계산된 x_n과 y_n에 대한 위상결과 값과 신호 발생 구조를 그림 2에 보인다.

혼돈시스템의 신호는 초깃값 x_0에 의해 x_1이 계산되고 다시 $x_2 .. x_n$이 계산되며, 그 결과 값은 $x_n \in [-2,2]$에 일정하게 분포되어 있어 전송되는 데이터를 암호화 하는데 효과적이다.

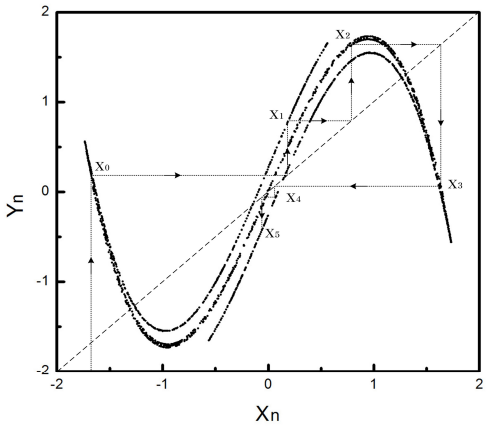

그림 2. Duffing-Map의 $X_n - Y_n$ 위상 그래프
Fig. 2 Phase space diagram of Duffing-Map

3.2. 보안 통신 프로토콜

우리는 3.1절에서 보인 Duffing-Map의 혼돈특성을 이용하여 그림 3과 같이 보안 통신 프로토콜을 제안한다. 제안된 내용 중 두 서버는 각각 다른 난수로 초기화하여 계산되고 단방향으로 되먹임 동기화 시켜 값이 일치되면 그 값을 대칭키로 하여 메시지를 전송하는 방법으로 단계별 처리 과정을 다음과 같이 보인다.

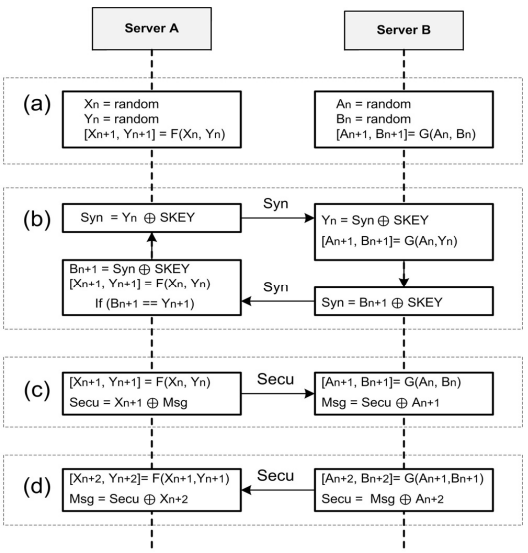

그림 3. 제안된 프로토콜의 구조
Fig. 3 Structure of proposed protocol

초기단계 (a). 두 서버의 $F(X_n, Y_n)$과 $G(A_n,B_n)$는 각각 다른 난수를 초기 값으로 계산하여 대칭키 X_n 과 A_n은 일치하지 않은 상태이다.

동기화단계 (b). 두 서버의 대칭키를 일치시키기 위해 단방향 되먹임으로 동기화를 시킨다. 두 서버에 사전에 공유된 비밀 키 $SKEY$를 이용하여 $F(X_n, Y_n)$에서 계산된 Y_n값을 $Syn = Y_n \oplus SKEY$로 계산하여 전송한다. 수신된 Syn값을 $Y_n = Syn \oplus SKEY$로 계산하여 y_n값을 $G(A_n,B_n)$에 되먹임 하여 계산한다. 계산된 B_{n+1}값을 $SKEY$로 처리하여 다시 전송하면 송신측에서 Y_{n+1}과 B_{n+1}이 일치하는지를 계산하여 동기화 여부를 결정한다.

통신단계 (c). 동기화가 성립되면 Msg를 대칭키 X_n을 이용하여 $Secu = X_n \oplus Msg$로 계산하여 암호화된 $Secu$를 전송한다. 수신측에서는 수신된 $Secu$를 $Msg = Secu \oplus A_{n+1}$하여 원문 Msg를 복호화 한다.

검증단계 (d). 수신측은 복호화 된 Msg를 검증하기 위해 $G(A_{n+1},B_{n+1})$로 계산된 A_{n+2}로 암호화 하여 전송하고 송신측에서도 $F(X_{n+1}, Y_{n+1})$로 계산된로 X_{n+2}검증하여 Msg의 변조 유무와 동기화 유지 여부를 판단한다.

3.3. 제안된 프로토콜 시뮬레이션

우리는 제안된 보안 프로토콜의 암호화 결과를 가시화시키기 위해 임의의 JPG 이미지파일을 제안된 프로토콜을 통해 서버로 전송하는 시뮬레이션을 실행하고 중간에서 무단 도청된 메시지를 JPG 이미지로 생성하여 원본과 도청된 이미지를 각각 히스토그램과 함께 그림 4에 보인다.

(a)는 전송시킨 원본이미지이고, (b)는 원본이미지의 히스토그램, (c)는 무단 도청된 이미지이고 (d)는 그것의 히스토그램이다. 도청된 데이터로 원본 데이터를 식별하기 불가능 한 것을 확인 할 수 있고 암호화 정보를 확인하기 위해 도청된 이미지에 대한 상관계수를 측정 하였다.상관 계수 측정은 이미지의 픽셀을 변경하며 진행 했고 관련된 내용을 식 (2)에 보인다.

$$\rho_{x,y} = \frac{Cov(r_x, r_y)}{\sigma_x \sigma_y} \quad (2)$$

식 (2)에 보이는 $Cov(r_x, r_y)$는 공분산 계산 값이고, σ_x와 σ_y는 각각 x와 y의 표준편차 값이다.

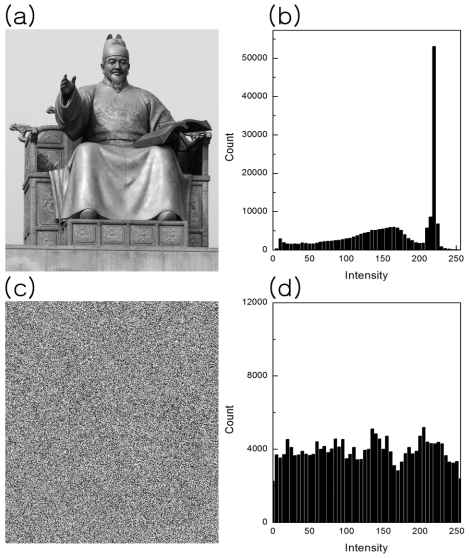

그림 4. 제안된 프로토콜의 결과 값
Fig. 4 Application of proposed protocol

계산된 결과 값을 표 1에 보이고 결과 값으로 암호화 정도가 높다는 것을 확인 할 수 있다.

표 1. 원본이미지와 암호화된 이미지의 상관계수
Table 1. Correlation coefficient of the original image and ciphered image

Direction of Adjacent Pixles	Original Image	Ciphered Image
Horizontal	0.54	0.001
Vertical	0.65	0.002
Diagonal	0.66	0.001

Ⅳ. 안정성 분석

본 장에서는 우리가 제안한 보안 프로토콜에 대한 전반적인 요구사항 과 공격방법에 대한 대응책 및 특

성을 비교 분석한다.

4.1. 기밀성(Confidentiality)

데이터 통신에 사용되는 모든 정보는 도청에 이용되지 않도록 암호화 되어 있어야 한다. 우리가 제안하는 프로토콜은 혼돈시스템에서 발생되는 유사난수 신호를 대칭키로 사용하여 암호화 하므로 도청공격으로 무단 수집된 신호로는 전송된 원본 데이터를 복원 할 수 없어 정보 은폐에 효과적이다. 혼돈시스템의 신호는 재생성이 가능하여 결정된 난수라고 하지만 혼돈시스템의 초깃값과 매개변수를 정확히 구성하지 못하면 같은 난수를 생성 할 수 없어 데이터 통신의 기밀성이 유지된다.

4.2. 무결성(Integrity)

우리가 제안한 통신 프로토콜은 무결성을 보장하기 위한 단방향 인증이 가능한 특징을 가지고 있다. 혼돈시스템의 계차방정식을 암호화에 사용하기 때문에 x_{n+1}은 x_n에 의해 계산된다. 전송되는 $x_{n+1} \oplus Data$ 값이 스푸핑 공격이나 재전송 공격을 받았을 때 x_n의 단방향 연관성계산으로 변조 유무를 확인 할 수 있어 무결성을 보장해 준다.

4.3. 가용성(Availability)

도청공격으로 대량의 데이터를 무단 획득하여도 혼돈시스템의 유사난수로 암호화된 데이터이므로 혼돈계의 종류, 특성, 초깃값 등을 정확히 파악하기 전에는 같은 값을 계산할 수 없어 외부 공격으로부터 메시지를 보호할 수 있고, 서비스 거부공격에 대해서도 x_{n+1}과 x_n의 계산으로 공격성 접근을 제안 하여 가용성을 보장한다.

Ⅴ. 결 론

인터넷과 개인용 스마트 단말기들의 발전으로 네트워크상에서 전송되는 데이터의 양이 대량화 되고 있다. 이런 양적인 발전과 함께 전송되는 데이터의 안전성 보장에 대한 관심도 늘어나고 있는 추세이다. 우리는 이런 데이터의 보호를 위해 기존의 암호화 방법이 아닌 새로운 방법으로 혼돈시스템의 단방향 동기화를 암호화에 적용시켰다. 혼돈시스템에서 발생되는 신호는 초깃값에 민감하고 발생되는 신호가 난수와 유사하여 예측이 불가능하다는 특징을 가지고 있다. 우리가 제안한 방법은 이런 특성의 신호를 발생하는 송신측과 수신측을 동기화 시켜 같은 시점에 동일화 신호를 대칭키로 사용하는 암호화 방법이다. 제안된 프로토콜의 결과를 가시화시키기 위해 이미지를 전송하고 무단 도청하는 시뮬레이션을 실행하고 그 결과를 보였다. 제안된 방법이 기존에 사용되고 있는 상용 암호화 알고리즘에 비해 안전성이나 속도 면에서 완전한 검증이 이루어지지는 않았지만 새로운 암호화 방법과 혼돈신호를 이용한 암호화 방법을 연구하는 연구자들에게 좋은 응용 연구가 되고 이후 새로운 연구 결과의 초석이 될 것으로 생각 된다.

References

[1] C.-S. Lee, “A Study on MD5 Security Routing based on MANET,“ *J. of the Korea Institute of Electronic Communication Sciences*, vol. 7, no, 4, 2012. pp. 797-780.

[2] C.-K. Lee and W.-Y. Jeong, “A Study on Authentication Algorithm for NFC Security Channel,“ *J. of the Korea Institute of Electronic Communication Sciences*, vol. 7, no, 4, 2012. pp. 805-810.

[3] S.-J. Park and J.-H. Park, “Current Status and Analysis of Domestic Security Monitoring Systems,“ *J. of the Korea Institute of Electronic Communication Sciences*, vol. 9, no. 2, 2014. pp. 261-266.

[4] F. C. M. Lau and C. K. Tse, *Chaos-Based Digital Communication Systems.* Berlin: Springer, 2003.

[5] H. Zhang, D, Liu, and Z, Wang, *Controlling Chaos.* London: Springer, 2009.

[6] L. Kocarev and S. Lian, *Chaos-Based Cryptography.* Berlin: Springer, 2011.

[7] G.-S. Yim and H.-S. Kim, "Chaos-based Image Encryption Scheme using Noise-induced Synchronization," *J. of the Korea Society of Computer*

and Information, vol. 13, no. 5, 2008, pp. 155-162.

[8] G.-S. Yim, "Design and Implementation of Image Encryption Method for Multi-Parameters Chaotic System," *Korea Information Assurance Society*, vol. 8. no. 3, 2008, pp. 57-64.

[9] H.-S. Kim and G.-S. Yim, "Design of a digital photo frame for close-range security using the chaotic signals synchronization," *J. of the Korea Society of Computer and Information,* vol. 16, no. 2, 2011, pp. 201-206.

[10] H. G. Schuster, *Deterministic Chaos an Introduction. 2nd*, Weinheim: VCH, 1988.

[11] G. P. Williams, *Chaos Theory Tamed.* London: Taylor & Francis, 1997.

[12] E. Ott, *Chaos in dynamical systems.* New York: Cambridge University Press, 1993.

[13] G. L. Baker and J. P. Gollub, *Chaotic Dynamics 2nd.* New York: Cambridge University Press, 1996.

[14] A. H. Nayfeh and B. Balachandran, *Applied Nonlinear Dynamics.* Toronto: Wiley-Interscience, 1995.

[15] J. C. Yen and J. I. Guo "A new chaotic key-based design for image encryption and decryption," *The 2000 IEEE Int. Symp. on Circuits and Systems*, Geneva, Switzerland, May 2000, pp. 49-52.

[16] H. E. Ahmed, H. M. Kalash, and O. S. Farag Allah, "An Efficient Chaos-Based Feedbacks Stream Cipher for Image Encryption and Decryption," *Information,* vol. 31, 2007. pp. 121-129.

[17] F. Fu, Z. Zhang, Y. Chen, and X. Wang, "An Improved Chaos-Based Image Encryption Scheme," *Int. Conf. on Computer Science 2007*, Beijing, China, June 2007, pp. 575-582.

저자 소개

조창호(Chang-Ho Cho)

1982년 서울대학교 대학원 물리학과 졸업(이학석사)
1988년 서울대학교 대학원 물리학과 졸업(이학박사)
1985년~현재 배재대학교 전기공학과 교수
※ 관심분야 : 시계열분석, 광학의료기기, 자동화장비, 임베디드시스템

임거수(Geo-Su Yim)

1998년 배재대학교 대학원 물리학과 졸업(이학석사)
2004년 서강대학교 대학원 물리학과 졸업(이학박사)
2008년~현재 배재대학교 전기공학과 교수
※ 관심분야 : 시계열분석, 신호처리, 빅데이타 분석, FPGA 비젼 제어